



SPECIFICHE FUNZIONALI API DI CONSULTAZIONE DOMICILI DIGITALI, INDIRIZZI IMPRESE E LEGALE RAPPRESENTANTE

API di consultazione per PagoPA

Redatto da	InfoCamere		
Versione	6	Data Versione:	26/ 12/ 2022
Descr. modifiche	Aggiornamento URL per servizio indirizzo attestazione pec e legale rappresentante oltre ai casi di test censiti nell'appendice		
Motivazioni			

Acronimi e glossario

Definizione / Acronimo	Descrizione
LG	Linee Guida
ModI	Modello di Interoperabilità della PA
Tecnologia REST	Modalità per implementare servizi basati sul protocollo HTTP che operano sulle risorse definite secondo la sintassi e la semantica previste per le URI e, sulle quali, si opera invocando delle operazioni (HTTP method) che agiscono su di esse.

Riferimenti

[LG INTEROPERABILITA']	Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni https://www.agid.gov.it/sites/default/files/repository_files/line_e_guida_interoperabilit_tecnica_pa.pdf
[LG SICUREZZA API]	Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici https://www.agid.gov.it/sites/default/files/repository_files/line_e_guida_tecnologie_e_standard_sicurezza_interoperabilit_api_sistemi_informatici.pdf

Sommario

1 Introduzione	3
2 Contesto	4
3 Descrizione delle API	6
3.1 API di estrazione	6
3.1.1 Servizio di autenticazione	6
3.1.2 Richiesta elenco PEC per codice fiscale o partita IVA	7
3.1.3 Recupero elenco PEC per codice fiscale o partita IVA	8
3.1.4 Recupero dell'indirizzo della sede legale dell'impresa	9
3.1.5 Attestazioni PEC	10
3.1.6 Legale rappresentante (puntuale)	11
3.1.7 Legale rappresentante (elenco)	12
3.3 Modelli di risposta	13
3.3.1 Servizio richiesta elenco PEC	13
3.3.2 Servizio download elenco PEC	14
3.3.3 Servizio sede d'impresa	15
3.3.4 Servizio di attestazione PEC	16
3.3.5 Servizio legale rappresentante (puntuale)	17
3.3.6 Servizio legale rappresentante (elenco)	17
5 Caratteristiche tecniche	18
5.1 Web Service	18
5.2 Specifiche di interoperabilità	19
5.2.1 Scope dei servizi	20
5.2.2 Ambiente di collaudo	20
5.3 Trust tra le parti	20
6 Livelli di servizio	21
6.1 Volumi e Carico	21
6.2 Orari di servizio	21
6.3 Uptime	22
6.4 Interventi di manutenzione	22
6.5 Sonde e Monitoraggio	22
6.6 Alta affidabilità	22
6.7 Disaster Recovery	22
6.8 Sicurezza	23

7 Appendice	23
7.1 Casi di test	23

1 Introduzione

Il documento ha l'obiettivo di descrivere le API pubbliche per dare seguito alle estrazioni dei dati dell'indice INI-PEC e del Registro delle Imprese.

Nello specifico i dati di interesse sono seguenti argomenti:

- indirizzo PEC dell'impresa;
- indirizzo PEC del professionista;
- indirizzo della sede legale dell'impresa;
- attestazioni di domicilio digitale alla data;
- legale rappresentante dell'impresa.

2 Contesto

PagoPA nell'ambito dell'attività di invio delle notifiche è interessata ad ottenere i dati sopra indicati.

In particolare, a fronte di un codice fiscale d'impresa (oppure partita IVA) o di professionista, si richiede l'indirizzo di posta elettronica certificata (di seguito PEC). Il **domicilio digitale** è l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata (di seguito PEC) o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS, valido ai fini delle comunicazioni elettroniche aventi valore legale ai sensi dell'articolo 1, comma 1, lettera n-ter del CAD.

Il servizio di attestazioni del domicilio digitale alla data è un servizio dedicato che consente di ottenere un'attestazione firmata del domicilio di una certa posizione ad una determinata data.

Il servizio di verifica del legale rappresentante è un servizio dedicato che, data una coppia costituita da codice fiscale della persona (fisica o giuridica) e codice fiscale dell'impresa, verifichi che la persona sia, o meno, legale rappresentante dell'impresa. Lo stesso servizio se invocato solo con il codice fiscale della persona, risponde con l'elenco delle imprese rappresentate.

I servizi sono conformi alle linee guida pubblicate da AgID ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e s.m.i. recante il "Codice dell'Amministrazione digitale" (CAD) il tutto mediante API, conformi alle [LG INTEROPERABILITA'] e delle [LG SICUREZZA API], per dare seguito ad estrazioni puntuali.

L'accesso puntuale avviene attraverso l'uso di uno dei seguenti parametri di ricerca:

Servizio PEC:

- *codice fiscale/partita IVA*: consente di ottenere il domicilio digitale ad esso corrispondente al momento della consultazione;

Servizio sede legale:

- *codice fiscale/partita IVA*: consente di ottenere l'indirizzo della sede legale dell'impresa al momento della consultazione;

Servizio attestazioni PEC:

- codice fiscale e data: produzione delle attestazioni del domicilio digitale alla data.

Servizio legale rappresentante:

- codice fiscale della persona e codice fiscale dell'impresa: consente di verificare se c'è corrispondenza tra i due codici fiscali;



- codice fiscale della persona: consente di ottenere la lista delle imprese in cui la persona ha una carica di rappresentanza.

L'accesso a tali funzionalità prevede autenticazione dei soggetti di cui all'articolo 2, comma 2, lettere a) e b) del CAD.

3 Descrizione delle API

I servizi sono erogati mediante API realizzate in conformità con il nuovo Modello di Interoperabilità (ModI) delle Pubbliche Amministrazioni definito da AgID.

In conformità con le Linee Guida pubblicate da AgID in materia di tecnologie e standard da utilizzare nella realizzazione dei sistemi informatici e nel garantire la sicurezza delle transazioni digitali, le API hanno le seguenti caratteristiche:

- sono esposte in modalità REST;
- utilizzano il protocollo di comunicazione HTTPS;
- l'autenticazione è gestita attraverso l'utilizzo di certificati digitali il cui standard di riferimento è rappresentato dall'X.509 e che definisce il formato dei certificati a chiave pubblica (PKC) e delle autorità di certificazione (CA);
- dispongono di un ambiente di collaudo distinto da quello di produzione;
- utilizzano un certificato di Dominio (valevole solo all'interno del Dominio di Interoperabilità) per l'ambiente di collaudo ed un certificato rilasciato da una CA Qualificata per l'ambiente di produzione;
- La fiducia delle interazioni erogatore-fruttore (ONBOARDING) è assicurata dalla costituzione di un trust tra essi al fine di riconoscere la validità dei certificati digitali utilizzati per assicurare la sicurezza delle comunicazioni realizzate tramite API;
- le diverse versioni delle API sono tracciate allo scopo di consentire evoluzioni non distruttive (versioning).

A livello applicativo l'utilizzo dei certificati si traduce in:

Autenticazione dell'utente tramite firma dell'hash dei dati significativi della chiamata con un certificato digitale associato all'utente (JWT Token);

Criptazione dei dati trasmessi tramite chiave asimmetrica.

I servizi sono descritti di seguito. Ognuno deve essere invocato con i parametri richiesti.

3.1 API di estrazione

Tutte le API esposte saranno documentate secondo standard OpenAPI 3.0

3.1.1 Servizio di autenticazione

Per il servizio di autenticazione si faccia riferimento al capitolo [“5.2 Specifiche di interoperabilità”](#) si tenga presente che ogni servizio ha uno scope dedicato (“Scope OAuth per accesso”) che deve essere richiesto in fase di autenticazione per avere accesso alla specifica API richiesta.

Per gli endpoint di contatto:

- ambiente di collaudo:
https://icapiscl.infocamere.it/ic/ce/wspa/wspa/rest/authentication?client_id=a7e152cac460917f3123cc2410f5a8d2

- ambiente di produzione: *url* (sarà fornito)

3.1.2 Richiesta elenco PEC per codice fiscale o partita IVA

POST		https://icapisl.infocamere.it/ic/ce/wspa/wspa/rest/richiestaElencoPec?client_id=a7e152cac460917f3123cc2410f5a8d2
Consente di richiedere un elenco di PEC delle imprese oppure del professionista corrispondente all'elenco fornito in input		
Authorization: token OAuth		
Scope OAuth per accesso: pec-pa		
<i>Parametri di input</i>		
<i>Nome</i>	<i>Tipo</i>	<i>Descrizione</i>
elencoCf	multipart/form-data	Elenco di codici fiscali o partite IVA da ricercare (obbligatorio). Massimo 10.000 codici fiscali per volta. Modello di richiesta JSON [INPUT] descritto al paragrafo 3.3.1.
<i>Risposte HTTP</i>		
<i>Codice</i>	<i>Descrizione</i>	
200	OK JSON di risposta che restituisce l'identificativo della richiesta da evadere in differita Modello di risposta JSON [PEC] descritto al paragrafo 3.3.1.	
400	Bad Request	
401	Unauthorized	
404	Not Found	
500	Internal Server Error	
503	Service Unavailable	

3.1.3 Recupero elenco PEC per codice fiscale o partita IVA

GET		https://icapiscl.infocamere.it/ic/ce/wspa/wspa/rest/getElencoPec/{id identificativoRichiesta}?client_id=a7e152cac460917f3123cc2410f5a8d2
Consente di ottenere un elenco di PEC delle imprese oppure del professionista corrispondente all'elenco di codice fiscale richiesti		
Authorization: token OAuth		
Scope OAuth per accesso: pec-pa		
<i>Parametri di input</i>		
<i>Nome</i>	<i>Tipo</i>	<i>Descrizione</i>
identificativoRichiesta	path	Identificativo della richiesta di elenco PEC restituito dal servizio descritto nel paragrafo precedente
<i>Risposte HTTP</i>		
<i>Codice</i>	<i>Descrizione</i>	
200	OK Il servizio risponde con un allegato che contiene l'elenco richiesto Modello di risposta JSON [ELENCO PEC] descritto al paragrafo 3.3.2.	
400	Bad Request	
401	Unauthorized	
404	Not Found - Il servizio risponde con questo codice anche se la richiesta non è ancora stata evasa	
500	Internal Server Error	
503	Service Unavailable	

3.1.4 Recupero dell'indirizzo della sede legale dell'impresa

POST		https://icapisl.infocamere.it/ic/ce/wspa/wspa/rest/sede/{cf}?client_id=a7e152cac460917f3123cc2410f5a8d2
Consente di ottenere l'indirizzo della sede legale dell'impresa al codice fiscale al momento della consultazione.		
Authorization: token OAuth		
Scope OAuth per accesso: sede-impresa-pa		
<i>Parametri di input</i>		
<i>Nome</i>	<i>Tipo</i>	<i>Descrizione</i>
cf	path	codice fiscale o partita IVA da ricercare (obbligatorio)
<i>Risposte HTTP</i>		
<i>Codice</i>	<i>Descrizione</i>	
200	OK JSON di risposta che restituisce l'indirizzo della sede legale dell'impresa Modello di risposta JSON [SEDE] descritto al paragrafo 3.3.2.	
400	Bad Request	
401	Unauthorized	
404	Not Found	
500	Internal Server Error	
503	Service Unavailable	

3.1.5 Attestazioni PEC

GET	https://icapisl.infocamere.it/ic/ce/wspa/wspa/rest/attestazioniPec/{cf}?data=<data>	
Consente di ottenere l’attestazione del domicilio digitale ad una certa data.		
Authorization: token OAuth		
Scope OAuth per accesso: pec-pa		
Parametri di input		
Nome	Tipo	Descrizione
cf	path	codice fiscale o partita IVA dell’impresa da ricercare (obbligatorio)
data	query	data di riferimento per la richiesta di attestazione del domicilio digitale (required = false)
Risposte HTTP		
Codice	Descrizione	
200	OK PDF firmato di risposta che reca l’attestazione del domicilio digitale alla data richiesta Modello di risposta PDF (in bozza) [ATTESTAZIONI PEC] descritto al paragrafo 3.3.3.	
400	Bad Request	
401	Unauthorized	
404	Not Found	
500	Internal Server Error	
503	Service Unavailable	

3.1.6 Legale rappresentante (puntuale)

GET	https://icapiscl.infocamere.it/ic/ce/wspa/wspa/rest/legaleRappresentante/{cfPersona}?cfImpresa={cfImpresa}	
Consente di verificare se il codice fiscale della persona risulta legale rappresentante dell’impresa passata come parametro		
Authorization: token OAuth		
Scope OAuth per accesso: lr-pa		
Parametri di input		
Nome	Tipo	Descrizione
cfPersona	path	codice fiscale della persona (obbligatorio)
cfImpresa	query	codice fiscale dell’impresa
Risposte HTTP		
Codice	Descrizione	
200	OK JSON di risposta che restituisce l’esito della verifica effettuata Modello di risposta [LEGALE RAPPRESENTANTE] descritto al paragrafo 3.3.4.	
400	Bad Request	
401	Unauthorized	
404	Not Found	
500	Internal Server Error	
503	Service Unavailable	

3.1.7 Legale rappresentante (elenco)

GET		https://icapiscl.infocamere.it/ic/ce/wspa/wspa/rest/listaLegaleRappresentante/{cfPersona}
Consente di ottenere la lista delle imprese rappresentate dal codice fiscale della persona (fisica o giuridica) passata come parametro		
Authorization: token OAuth		
Scope OAuth per accesso: lr-pa		
<i>Parametri di input</i>		
<i>Nome</i>	<i>Tipo</i>	<i>Descrizione</i>
cfPersona	path	codice fiscale della persona (obbligatorio)
<i>Risposte HTTP</i>		
<i>Codice</i>	<i>Descrizione</i>	
200	OK JSON di risposta che restituisce l'esito della verifica effettuata Modello di risposta [LEGALE RAPPRESENTANTE ELENCO] descritto al paragrafo 3.3.6.	
400	Bad Request	
401	Unauthorized	
404	Not Found	
500	Internal Server Error	
503	Service Unavailable	

3.3 Modelli di risposta

3.3.1 Servizio richiesta elenco PEC

[INPUT]
Location: <a href="https://<dominioOrganizzativo>/rest/spec/v1/richiestaElencoPec">https://<dominioOrganizzativo>/rest/spec/v1/richiestaElencoPec
Content-Type: application/json
<p>Request input file:</p> <pre> { "dataOraRichiesta": "<dataOra>", "elencoCf": [{ "cf": "<cf_{INPUT}>" }, { "cf": "<cf_{INPUT}>" }, { "cf": "<cf_{INPUT}>" }] }</pre>

[PEC]
Location: <a href="https://<dominioOrganizzativo>/rest/spec/v1/richiestaElencoPec">https://<dominioOrganizzativo>/rest/spec/v1/richiestaElencoPec
Content-Type: application/json
<p>Response body:</p> <pre> { "dataOraEstrazione": "<dataOra_{INPUT}>", "identificativoRichiesta": "<identificativoRichiesta_{INPUT}>" }</pre>

3.3.2 Servizio download elenco PEC

[ELENCO PEC]
Location: https://<dominioOrganizzativo>/rest/spec/v1/getElencoPec/{identificativoRichiesta}
Content-Type: application/json
<p>Response body:</p> <pre>{ "dataOraDownload": "<dataOra>", "identificativoRichiesta": "<identificativoRichiesta_INPUT>", "elencoPec": [{ "cf": "<cf_INPUT>", "pecImpresa": "<indirizzo_PEC>", "pecProfessionistas": [{ "pecProfessionista": "<indirizzo_PEC>" }, { "pecProfessionista": "<indirizzo_PEC>" }] }] }</pre>

3.3.3 Servizio sede d'impresa

[SEDE]
Location: <code>https://<dominioOrganizzativo>/rest/spec/v1/sede/{cf}</code>
Content-Type: application/json
<p>Response body:</p> <pre>{ "dataOraEstrazione": "<dataOra>", "cf": "<cf_{INPUT}>", "indirizzoLocalizzazione": { "denominazione": "<denominazione_{SEDE}>", "comune": "<comune_{SEDE}>", "provincia": "<siglaProvincia_{SEDE}>", "toponimo": "<toponimo_{SEDE}>", "via": "<nomeVia_{SEDE}>", "nCivico": "<numeroCivico_{SEDE}>", "cap": "<CAP_{SEDE}>" } }</pre>

3.3.4 Servizio di attestazione PEC

Di seguito un template di attestazione relativo al domicilio estratto alla data.



Oggetto: Esito risultante dalla consultazione dell'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata

Con riferimento alla Vostra richiesta relativa alla posizione xxxxxxxxxxxxxxxx , si attesta che, in data **01/08/2017**, alle ore **10:00**, l'esito risultante dall'accesso e consultazione dell'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata è stato il seguente:

- indirizzo PEC presente: xxxxxxxxx@pec.it

Luogo e data
Roma, 02/08/2017

per InfoCamere S.c.p.A.

Andrea Acquaviva

3.3.5 Servizio legale rappresentante (puntuale)

[LEGALE RAPPRESENTANTE]
Location: <a href="https://<dominioOrganizzativo>/rest/spec/v1/legaleRappresentante/{cfPersona}?cfImpresa=<cfImpresa>">https://<dominioOrganizzativo>/rest/spec/v1/legaleRappresentante/{cfPersona}?cfImpresa=<cfImpresa>
Content-Type: application/json
Response body: <pre>{ "dataOraEstrazione": "<dataOra>", "cfPersona": "<cfPersona<sub>INPUT</sub>>", "cfImpresa": "<cfImpresa<sub>INPUT</sub>>", "esitoVerifica": "<esitoVerifica<sub>LR</sub>>" }</pre>

3.3.6 Servizio legale rappresentante (elenco)

[LEGALE RAPPRESENTANTE ELENCO]
Location: <a href="https://<dominioOrganizzativo>/rest/spec/v1/legaleRappresentante/{cfPersona}">https://<dominioOrganizzativo>/rest/spec/v1/legaleRappresentante/{cfPersona}
Content-Type: application/json
Response body: <pre>{ "dataOraEstrazione": "<dataOra>", "cfPersona": "<cfPersona<sub>INPUT</sub>>", "elencoImpreseRappresentate": [{ "cfImpresa": "<cfImpresa<sub>LR</sub>>", "denominazione": "<denominazione<sub>LR</sub>>" }, { "cfImpresa": "<cfImpresa<sub>LR</sub>>", "denominazione": "<denominazione<sub>LR</sub>>" }] }</pre>

5 Caratteristiche tecniche

5.1 Web Service

Si espongono in forma di web services di tipo REST e sono “stateless” ovvero non hanno memoria di stato: sono servizi puntuali che non tracciano alcuna sessione riferita all'utente e sono indipendenti dall'organizzazione dei dati dell'interfaccia web, quindi, sono orientati al massimo riutilizzo. Gli obiettivi coperti da questo tier sono molteplici:

- implementare la business logic;
- interfacciarsi con le banche dati istituzionali e interagire con la banca dati specifica del domicilio digitale;
- interfacciarsi con servizi interni ed esterni.

Api Interface

L'API Interface mette a disposizione ai soggetti autorizzati, mediante cooperazione A2A, servizi API che permettono l'interrogazione dell'indice dei domicili digitali. I servizi sono orientati a fornire le informazioni richieste interrogando i servizi di back-end. L'API Interface sarà implementata seguendo le linee guida definite da AgID e regolamentate all'art. 71 del CAD.

Tecnologie di riferimento

Il sistema è realizzato utilizzando un'API-Centric Architecture.

Nello specifico:

- lato server la base applicativa è strutturata con un sistema “multi-tier” con un front-end, un back-end e un layer di persistenza (database). L'applicazione è distribuita nel “Cloud” privato di InfoCamere, un sistema cluster di Application Server dedicati, in alta affidabilità e scalabilità, a cui sono anteposti dei web server per il bilanciamento e la gestione delle risorse statiche. Il cluster a sua volta è mosso da un sistema di virtualizzazione, diviso su due o più rami distinti a futuro supporto della “business continuity”. Il tutto è organizzato per poter scalare rapidamente, garantire una alta disponibilità del servizio e tolleranza ai guasti, ed è coperto dal sistema di Disaster Recovery;
- il sistema è dotato di una propria base dati relazionale che rappresenta l'indice nazionale dei domicili digitali;
- per l'estrazione dati e l'accesso alle banche dati istituzionali il sistema fa affidamento a vari servizi interni condivisi acceduti tramite un API Manager che ne monitora e controlla gli accessi;
- per l'interazione con i servizi messi a disposizione da soggetti terzi esterni il sistema fa affidamento su interfacce API condivise. Ad esempio il sistema utilizza i servizi per la verifica dei domini di posta elettronica certificata resi disponibili da

AgID o altri servizi per la verifica degli indirizzi di posta elettronica certificata eventualmente forniti dai provider PEC.

5.2 Specifiche di interoperabilità

Il modello di interoperabilità, definito nelle [LG INTEROPERABILITA'], prevede l'interazione tra il soggetto Erogatore e il soggetto Fruitore per mezzo degli e-service realizzati dall'Erogatore.

La comunicazione tra Fruitore ed Erogatore avviene mediante API REST conformi alle [LG INTEROPERABILITA'] e alle [LG SICUREZZA API].

In particolare viene utilizzato OAuth 2.0 con Grant Type di tipo "Client Credential" secondo l'RFC 6749¹.

Per il riconoscimento del client e l'assegnazione del "access_token", è stato scelto il flow con Grant Type di tipo "Client Credential". In particolare si è scelto di seguire lo standard OpenID Connect (OIDC) 1.0 con riferimento alla modalità definita "private_key_jwt": in sostanza il client presenta via HTTPS POST all'Authorization server uno specifico JWT firmato con un proprio certificato, che ne attesta l'identità. Per i dettagli di questo protocollo comunicativo si faccia riferimento allo standard di riferimento già citato.

Per il certificato in questione prevediamo l'utilizzo di un certificato digitale rilasciato da una CAQ (standard "QSeal" eIDAS descritto in ETSI EN 319 412-1), come indicato nel prossimo paragrafo "[5.3 Trust tra le parti](#)".

InfoCamere provvederà alla consegna di un'identificativo (client_id) che dovrà essere usato secondo le specifiche di protocollo già indicate.

In particolare, secondo specifiche, il JWT inviato in post contiene nel payload, almeno:

- "iss" e "sub": entrambi valorizzati al "client_id";
- "aud": valorizzato all'url dell'endpoint per il rilascio token dell'authorization server, che verrà comunicato;
- "jti": identificativo unico per il token;
- "exp": tempo di scadenza oltre il quale il token non può essere accettato;

Il JWT header deve indicare esplicitamente:

- "x5c": la catena di trust codificato in base64;
- "alg": algoritmo di firma utilizzato, nella fattispecie "RS256";
- "typ": "jwt";
- "use": "sig";

¹ <https://www.ietf.org/rfc/rfc6749.txt>



Il token deve avere una scadenza massima di 10 minuti, consigliata 30 secondi.

Nella chiamata POST bisogna indicare il parametro scope valorizzandolo con l'elenco degli scope² associati alle singole API per cui si richiede l'accesso.

5.2.1 Scope dei servizi

Richiesta elenco PEC: **pec-pa**

Recupero elenco PEC: **pec-pa**

Attestazioni PEC: **pec-pa**

Recupero dell'indirizzo della sede legale dell'impresa: **sede-impresa-pa**

Legale rappresentante (puntale): **lr-pa**

Legale rappresentante (elenco): **lr-pa**

5.2.2 Ambiente di collaudo

InfoCamere prevede di mantenere un ambiente di collaudo separato rispetto a quello di produzione, al quale si potrà accedere facendo riferimento da un "client_id", che verrà fornito, utilizzando lo stesso certificato QSeal dell'ambiente di produzione.

5.3 Trust tra le parti

Per assicurare l'autenticazione/autorizzazione dei client dei soggetti di cui all'articolo 2, comma 2, lettere a) e b) del CAD, gli stessi si dotano di un Electronic Seal Certificates, ai sensi del Regolamento (UE) n. 910/2014, che identificano il soggetto giuridico a cui il sigillo è associato, abilitando la determinazione dell'origine, della correttezza e dell'integrità dei messaggi oggetto delle interazioni.

Nello specifico i soggetti di cui all'articolo 2, comma 2, lettere a) e b) del CAD richiedono alla Certification Authority qualificata il popolamento degli OID 2.5.4.97 organizationIdentifier e, se del caso, dell'OID 2.5.4.11 organizationalUnitName nel rispetto di quanto disposto al paragrafo "6.1.2 Object identifier per l'identificazione delle pubbliche amministrazioni" delle [LG SICUREZZA API].

I soggetti di cui all'articolo 2, comma 2, lettere a) e b) del CAD utilizzano gli Electronic Seal Certificates per la firma dei token JWT di autenticazione/autorizzazione.

Alla ricezione delle request si provvede ad autorizzare il client richiedente assicurando, oltre alla verifica della validità dell'Electronic Seal Certificates utilizzato dal client richiedente e

² gli elementi dell'elenco vanno separati dal carattere spazio, che ne rispetto dello standard URL, va rappresentato con la sequenza di caratteri %20

della CAQ emittente, all'attuazione di quanto disposto al paragrafo "6.1.2.3 Verifica associazione di certificato X.509 ad una pubblica amministrazione" delle [LG SICUREZZA API].

6 Livelli di servizio

6.1 Volumi e Carico

Il servizi illustrati nei paragrafi precedenti, avranno i seguenti SLA:

Servizio	SLA	Tempo di risposta medio
Servizio indirizzo INI-PEC	600.000/giorno	24h
Servizio sede d'impresa	900/min 400.000/giorno	0,8 sec/chiamata
Servizio attestazione PEC	-	-
Servizio legale rappresentante puntuale	900/min 400.000/giorno	0,5 sec/chiamata
Servizio legale rappresentante elenco	900/min, 400.000/giorno	0,5 sec/chiamata

I dati indicati fanno riferimento ad una configurazione standard con la possibilità di scalare il sistema sulla base dei volumi di carico indicati nella tabella precedente.

6.2 Orari di servizio

Per orario di servizio si intende l'intervallo in cui è presidiato il servizio applicativo. Lo stesso è disponibile h24 ma durante il presidio, tra le 8 e le 21 dal lunedì al sabato, festività escluse, qualsiasi fermo viene preso immediatamente in carico e risolto.

Tra le 21 e le 8 del mattino sono inoltre previste delle attività di manutenzione ordinaria che potrebbero provocare momentanee indisponibilità del servizio.

6.3 Uptime

L'uptime rappresenta il tempo di funzionamento del sistema informatico, e indica l'intervallo di tempo in cui esso è stato ininterrottamente funzionante ed attivo. La percentuale su base annua prevista è del 98%.

La indisponibilità dovuta ad interventi di manutenzione non viene considerata ai fini del calcolo dello SLA.

6.4 Interventi di manutenzione

InfoCamere avrà il diritto di effettuare ogni tipo di manutenzione sui sistemi informatici, impegnandosi sin d'ora a:

- comunicare per iscritto a PagoPA e pubblicamente sul sito, con un anticipo di 2 giorni, gli interventi di manutenzione programmata che comportino una interruzione dei servizi;
- comunicare per iscritto a PagoPA e pubblicare sul sito del servizio, con un preavviso compatibile con l'urgenza dell'attività, gli eventuali interventi di manutenzione straordinaria non programmata che comportino una interruzione dei servizi, fermo restando che, salvo casi eccezionali di forza maggiore;
- comunicare tempestivamente per iscritto a PagoPA e pubblicare sul sito del servizio o, qualora questo fosse indisponibile, tramite canali pubblici alternativi, ogni significativo malfunzionamento in corso.

6.5 Sonde e Monitoraggio

L'applicazione prevede un sistema a sonde per il monitoraggio della disponibilità del servizio.

6.6 Alta affidabilità

Il servizio sarà erogato in architettura logica e fisica di alta affidabilità e continuità operativa. A questo proposito InfoCamere ha ottenuto a dicembre 2018 la certificazione alla norma ISO 22301 che riguarda proprio la business continuity.

6.7 Disaster Recovery

Il sistema sarà sottoposto a Disaster Recovery garantendo l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi, a fronte di gravi emergenze che ne intacchino la regolare attività.

InfoCamere con il suo sito di DR, è in grado di ripristinare l'operatività di un servizio a fronte di un evento disastroso con un RPO di 24 ore ed un RTO di 72 ore calcolati a partire dal momento in cui viene dichiarata la situazione di disastro.

6.8 Sicurezza

InfoCamere si impegna ad erogare servizi che offrano ampie garanzie di sicurezza e conformità con le normative applicabili. A tal fine sono adottate le best practice di settore e vengono seguiti processi produttivi e gestionali controllati e certificati. InfoCamere si è dotata di un Sistema di Gestione della Sicurezza delle Informazioni certificato secondo lo standard ISO/IEC 27001 ed adotta politiche di sicurezza dirette al proprio personale e idoneamente contrattualizzate con le terze parti.

7 Appendice

Di seguito un esempio di token jwt per il servizio di autenticazione.

E' necessario in fase di onboarding comunicare la chiave pubblica del certificato di firma del JWT.

7.1 Casi di test

Casi di test per servizio sede d'impresa:

SEDE D'IMPRESA
02313821007
01501320442
00056530256
00070890256
00054710256

Casi di test per servizi sul legale rappresentante:

	LEGALE RAPPRESENTANTE	
	CF IMPRESA	CF PERSONA
ELENCO	01501320442	DLLDGI53T30I324E
PUNTUALE	---	DLLDGI53T30I324E
	---	MSSLGU51P10A087J